CLAIMS

What is claimed is:

1. A method for providing access control in a computing system environment, the method comprising the steps of:

receiving an access request;

selecting, based on the access request, a selected set of rules containing at least one rule from at least one master set of rules; and

performing at least one rule operation in the at least one rule in the selected set of rules to produce an access control decision until at least one of:

i) a rule operation including a disregard instruction is performed to limit performance of rule operations in the selected set of rules; and

ii) all rule operations in the selected set of rules that are applicable to the access control decision are performed.

2. The method of claim 1 wherein the step of performing includes the step of producing an access control decision indicating whether to allow access, on behalf of a requestor submitting the access request, to an resource in the computing system environment.

3. The method of claim 1 wherein the step of selecting includes the steps of:

determining an identity of the resource in the computing system environment to which access is requested in the access request; and

applying at least one filter operation, using the identity of the resource, for rules in the at least one master set of rules to produce the selected set of rules for use in determining the access control decision to the resource.

4. The method of claim 3 further including the step of:

determining a role identity of a requestor submitting the access request; and

wherein the step of applying applies the at least one filter operation, using the role identity of the requestor submitting the access request in combination with the identity of the resource, for rules in the at least one master set of rules to produce the selected set of rules for use in determining the access control decision to the resource.

5. The method of claim 1 wherein:

at least one rule in the selected set of rules contains a rule operation including an unconditional disregard instruction; and

wherein the step of performing includes the steps of:

performing less than all rule operations defined within the at least one rule in the selected set of rules by sequentially performing rule operations in each rule in the selected set of rules until the unconditional disregard instruction is performed thereby terminating the performance of any remaining rule operations in the selected set of rules.

6. The method of claim 5 wherein the selected set of rules is arranged hierarchically such that rules containing rule operations that are more specific are performed before rule operations that are more general.

7. The method of claim 1 wherein:

at least one rule in the selected set of rules contains a rule operation including a disregard instruction including disregard criteria; and

wherein the step of performing limits performance of rule operations in the selected set of rules by performing the disregard instruction containing disregard criteria such that at least one rule operation in any remaining rule operations in the selected set of rules is disregarded from further performance.

8. The method of claim 7 wherein the step of performing includes the steps of:

evaluating the disregard criteria against any remaining unperformed rule operations in the selected set of rules; and

marking any remaining unperformed rule operations in the selected set of rules that match the disregard criteria to be disregarded from further rule processing.

9. The method of claim 1 wherein the step of selecting includes the steps of:

determining an identity of a resource in the computing system environment to which access is requested in the access request; and

applying at least one filter operation, using the identity of the resource, for rules in the at least one master set of rules to produce the selected set of rules for use in determining the access control decision to the resource; and

wherein the method further includes the step of determining a role identity of a requestor submitting the access request; and

wherein the step of performing sequentially processes each rule operation in the selected set of rules using the role identity of the requestor submitting the access request in combination with the identity of the resource to determine if the requestor using the role identity can access the resource.

10. The method of claim 9 wherein:

at least one rule in the selected set of rules contains a rule operation including a disregard instruction including disregard criteria; and

wherein the step of performing limits performance of rule operations in the selected set of rules by performing the disregard instruction containing disregard criteria such that at least one rule operation in any remaining rule operations in the selected set of rules is disregarded from further performance.

11. The method of claim 10 wherein the step of performing includes the steps of:

evaluating the disregard criteria against any remaining unperformed rule operations in the selected set of rules; and

marking any remaining unperformed rule operations in the selected set of rules that match the disregard criteria to be disregarded from further rule processing.

12. The method of claim 10 wherein:

the selected set of rules is arranged hierarchically such that rules containing rule operations that are more specific are performed before rules containing rule operations that are more general such that placement of the disregard instruction in one of the at least one rules in the selected set of rules causes the step of performing to control an amount of access control provided to the requestor that submitted the access request for access to the resource.

13. The method of claim 10 wherein the disregard instruction is a conditional instruction that has a condition that must be met before the disregard instruction is performed.

14. The method of claim 1 wherein:

at least one rule in the selected set of rules contains a relation that defines a condition based on a group definition; and

wherein at least one of the steps of selecting and performing includes the step of:

performing the relation to determine if at least one of a requestor, an access, and a resource specified in the access request satisfy the condition based on the group definition.

15. A method for determining an authorization state of an access control system in a computing system environment, the method comprising the steps of:

receiving an access request;

determining at least one of:

i) an identity of the resource in the computing system environment to which the access request is directed; and

ii) a role identity of a requestor submitting the access request; and

applying at least one filter operation, based on at least one of the identity of the resource and the role identity of a requestor, to an at least one master set of rules to produce a list of rules to which the at least one filter operation matches in order to provide an indication of the authorization state of an access control system in a

computing system environment as related to at least one of the identity of the resource and the role identity of a requestor.

16. The method of claim 15 wherein the step of applying at least one filter operation applies a filter operation to determine what rules in the at least one master set of rules affect access to what resource in the computing system environment.

17. The method of claim 15 wherein the step of applying at least one filter operation applies a filter operation to determine what rules in the at least one master set of rules affect what at least one requestor can do to at least one resource in the computing system environment.

18. The method of claim 15 wherein the step of applying at least one filter operation applies a filter operation to determine access control operations that a requestor can do to at least one resource in the computing system environment.

19. A computer system configured to provide access control, the computer system comprising:

at least one input/output interface;

a processor;

a memory system encoded with an authorization program;

at least one authorization database;

an interconnection mechanism coupling the processor, the at least one input/output interface, the memory system, and the at least one authorization database;

wherein the at least one input/output interface receives an access request from a requestor and the processor performs the authorization program in the memory system to select, based on the access request, a selected set of rules containing at least one rule from at least one master set of rules maintained within the at least one authorization database; and

wherein the processor performs at least one rule operation in the at least one rule in the selected set of rules to produce an access control decision in the memory system until at least one of:

i) a rule operation including a disregard instruction is performed to limit performance of rule operations in the selected set of rules; and

ii) all rule operations in the selected set of rules that are applicable to the access control decision are performed

20. The computer system of claim 19 wherein the processor, via performance of the at least one rule operation, produces an access control decision indicating whether to allow access, on behalf of the requestor submitting the access request, to an resource in the computing system environment.

21. The computer system of claim 19 wherein:

the processor performs the authorization program to select the selected set of rules and to determine an identity of a resource in the computing system environment to which access is requested in the access request; and

the processor performs the authorization program to apply at least one filter operation from the at least one authorization database, using the identity of the resource, for rules in the at least one master set of rules to produce the selected set of rules for use in determining the access control decision to the resource.

22. The computer system of claim 18 wherein the processor performs the authorization program which determines a role identity of a requestor submitting the access request; and

wherein when the processor performs the authorization program to apply at least one filter operation, the authorization program applies the at least one filter operation, using the role identity of the requestor submitting the access request in combination with the identity of the resource, for rules in the at least one master set of rules to produce the selected set of rules for use in determining the access control decision to the resource.

23. The computer system of claim 22 wherein:

at least one rule in the selected set of rules in the authorization database contains a rule operation including an unconditional disregard instruction; and

wherein when the processor performs at least one rule operation, the processor performs less than all rule operations defined within the at least one rule in the selected set of rules by sequentially performing rule operations in each rule in the selected set of rules until the unconditional disregard instruction is performed thereby terminating the performance of any remaining rule operations in the selected set of rules.

24. The computer system of claim 23 wherein the selected set of rules is arranged hierarchically such that when the processor performs the authorization program, rules containing rule operations that are more specific are performed before rule operations that are more general.

25. The computer system of claim 19 wherein:

at least one rule in the selected set of rules contains a rule operation including a disregard instruction including disregard criteria; and

wherein the processor performs at least one rule operation to limit performance of rule operations in the selected set of rules by performing the disregard instruction containing disregard criteria such that at least one rule operation in any remaining rule operations in the selected set of rules is disregarded from further performance.

26. The computer system of claim 25 wherein the processor evaluates the disregard criteria against any remaining unperformed rule operations in the selected set of rules; and marks any remaining unperformed rule operations in the selected set of rules that match the disregard criteria to be disregarded from further rule processing.

27. The computer system of claim 19 wherein when the processor performs the authorization program to select a selected set of rules, the processor:

determines an identity of an resource to which access is requested in the access request; and

applies at least one filter operation, using the identity of the resource, for rules in the at least one master set of rules to produce the selected set of rules for use in determining the access control decision to the resource; and

wherein when the processor performs the authorization program, the processor determines a role identity of a requestor submitting the access request; and

wherein the processor sequentially processes each rule operation in the selected set of rules using the role identity of the requestor submitting the access request in combination with the identity of the resource to determine if the requestor using the role identity can access the resource.

28. The computer system of claim 27 wherein:

at least one rule in the selected set of rules contains a rule operation including a disregard instruction including disregard criteria; and

wherein the processor limits performance of rule operations in the selected set of rules by performing the disregard instruction containing disregard criteria such that at least one rule operation in any remaining rule operations in the selected set of rules is disregarded from further performance.

29. The computer system of claim 28 wherein the processor evaluates the disregard criteria against any remaining unperformed rule operations in the selected set of rules; and marks any remaining unperformed rule operations in the selected set of rules that match the disregard criteria to be disregarded from further rule processing.

30. The computer system of claim 28 wherein:

the selected set of rules is arranged hierarchically such that rules containing rule operations that are more specific are performed by the processor before rules containing rule operations that are more general such that placement of the disregard instruction in

one of the at least one rules in the selected set of rules causes the authorization program, when performed on the processor, to control an amount of access control provided to the requestor that submitted the access request for access to the resource.

31. The computer system of claim 28 wherein the disregard instruction is a conditional instruction that has a condition that must be met during processing by the processor before the disregard instruction is performed.

32. The computer system of claim 19 wherein:

at least one rule in the selected set of rules contains a relation that defines a condition based on a group definition; and

wherein when the processor performs at least one of the operations of selecting and performing, the processor performing the relation to determine if at least one of a requestor, an access, and a resource specified in the access request satisfy the condition based on the group definition.

33. A computer system for determining an authorization state of an access control system in a computing system environment, the computer system comprising:

at least one input/output interface;

a processor;

a memory system encoded with an authorization program;

at least one authorization database; and

an interconnection mechanism coupling the processor, the at least one input/output interface, the memory system, and the at least one authorization database;

wherein the at least one input/output interface receives an access request from a requestor and the processor performs the authorization program in the memory system to determine at least one of:

i) an identity of a resource to which the access request is directed; and

ii) a role identity of a requestor submitting the access request; and

wherein the processor further performs the authorization program to apply at least one filter operation, based on at least one of the identity of the resource and the role identity of a requestor, to an at least one master set of rules in the at least one authorization database to produce a list of rules to which the at least one filter operation matches in order to provide an indication of the authorization state of an access control system in a computing system environment as related to at least one of the identity of the resource and the role identity of a requestor.

34. The computer system of claim 33 wherein the processor applies a filter operation to determine what rules in the at least one master set of rules affect access to what resource.

35. The computer system of claim 33 wherein the processor applies a filter operation to determine what rules in the at least one master set of rules affect what at least one requestor can do to at least one resource.

36. The computer system of claim 33 wherein the processor applies a filter operation to determine access control operations that a requestor can do to at least one resource.

37. A method providing access control to an resource in a computing system environment, the method comprising the steps of:

receiving an access request from a requestor requesting access to a resource in the computing system environment;

determining a role identity associated with the requestor requesting access to the resource; and

processing the access request in relation to a rule set based on an identity of the resource in the computing system environment to which the requestor requested access and based on the role identity associated with the requestor to determine if the requestor is allowed access the resource; and

wherein the rule set includes a plurality of rules, each rule including a filter operation, and wherein the step of processing determines if a rule applies to the resource

in the computing system environment to which the requestor requested access based on the filter operation; and

wherein at least one rule in the rule set includes a disregard instruction, and wherein if the step of processing determines, based on the filter operation, that the rule including the disregard instruction applies to the resource in the computing system environment to which the requestor requested access, the step of processing processes the rule including the disregard instruction to limit performance of any remaining rule operations in the selected set of rules.

38. A computer program product having a computer-readable medium including computer program logic encoded thereon that when executed on a computer system provides a method for controlling access to a resource, and wherein when the computer program logic is executed on a processor in the computer system, the computer program logic causes the processor to perform the operations of:

receiving an access request;

selecting, based on the access request, a selected set of rules containing at least one rule from at least one master set of rules; and

performing at least one rule operation in the at least one rule in the selected set of rules to produce an access control decision until at least one of:

i) a rule operation including a disregard instruction is performed to limit performance of rule operations in the selected set of rules; and

ii) all rule operations in the selected set of rules that are applicable to the access control decision are performed.

39. The computer program product of claim 38 wherein when the computer program logic causes the processor to perform the operation of selecting, based on the access request, a selected set of rules, the computer program logic causes the processor to perform the operations of:

determining an identity of an resource in the computing system environment to which access is requested in the access request; and

applying at least one filter operation, using the identity of the resource, for rules in the at least one master set of rules to produce the selected set of rules for use in determining the access control decision to the resource; and

wherein the method further includes the step of determining a role identity of a requestor submitting the access request; and

wherein the step of performing sequentially processes each rule operation in the selected set of rules using the role identity of the requestor submitting the access request in combination with the identity of the resource to determine if the requestor using the role identity can access the resource.

40. The computer program product of claim 38 wherein at least one rule in the selected set of rules contains a rule operation including an unconditional disregard instruction; and

wherein when the computer program logic causes the processor to perform the operation of performing, the computer program logic causes the processor to perform the operation of:

performing less than all rule operations defined within the at least one rule in the selected set of rules by sequentially performing rule operations in each rule in the selected set of rules until the unconditional disregard instruction is performed thereby terminating the performance of any remaining rule operations in the selected set of rules.

41. The computer program product of claim 38 wherein at least one rule in the selected set of rules contains a rule operation including a disregard instruction including disregard criteria; and

wherein when the computer program logic causes the processor to perform the operation of performing, the operation of performing limits performance of rule operations in the selected set of rules by performing the disregard instruction containing disregard criteria such that at least one rule operation in any remaining rule operations in the selected set of rules is disregarded from further performance.

42. The computer program product of claim 41 wherein when the computer program logic causes the processor to perform the operation of performing, the computer program logic causes the processor to perform the operations of:

evaluating the disregard criteria against any remaining unperformed rule operations in the selected set of rules; and

marking any remaining unperformed rule operations in the selected set of rules that match the disregard criteria to be disregarded from further rule processing.

43. A computer program product having a computer-readable medium including computer program logic encoded thereon that when executed on a computer system provides a method for determining an authorization state of an access control system in a computing system environment, wherein when the computer program logic is executed on a processor in the computer system, the computer program logic causes the processor to perform the operations of::

receiving an access request;

determining at least one of:

i) an identity of the resource in the computing system environment to which the access request is directed; and

ii) a role identity of a requestor submitting the access request; and

applying at least one filter operation, based on at least one of the identity of the resource and the role identity of a requestor, to an at least one master set of rules to produce a list of rules to which the at least one filter operation matches in order to provide an indication of the authorization state of an access control system in a computing system environment as related to at least one of the identity of the resource and the role identity of a requestor.

44. A computer program product having a computer-readable medium including computer program logic encoded thereon that when executed on a computer system provides a method for controlling access to resources, and wherein when the computer

program logic is executed on the processor, the computer program logic causes the processor to perform the operations of:

receiving an access request from a requestor requesting access to a resource in a computing system environment;

determining a role identity associated with the requestor requesting access to the resource; and

processing the access request in relation to a rule set based on an identity of the resource in the computing system environment to which the requestor requested access and based on the role identity associated with the requestor to determine if the requestor is allowed access to the resource; and

wherein the rule set includes a plurality of rules, each rule including a filter operation, and wherein the step of processing determines if a rule applies to the resource in the computing system environment to which the requestor requested access based on the filter operation; and

wherein at least one rule in the rule set includes a disregard instruction, and wherein if the step of processing determines, based on the filter operation, that the rule including the disregard instruction applies to the resource in the computing system environment to which the requestor requested access, the step of processing processes the rule including the disregard instruction to limit performance of any remaining rule operations in the selected set of rules.

45. A method for controlling applicability of rule operations in a rule-based access control system, the method comprising the step of:

selecting at least one rule for performance to determine an access control decision; and

performing a rule operation in the at least one rule, the rule operation including a disregard instruction that when performed, causes non-performance of at least one other rule operation in at least one rule that is selected for performance to determine the access control decision.